In the claims:

All of the claims standing for examination are presented below with appropriate status indication.

1. (Currently amended) A method for authenticating a user and securing an online transaction over a telephone, comprising:

(a) connecting a smart card having a conventional ISO 7816 six pad array and first circuitry to operate as a conventional smart card, further comprising second circuitry enabled to produce a modulated voltage signal modulated in a manner to produce an identification sequence stored on the smart card and associated with a specific person, on one otherwise unused pad once each time the Rst (reset pad) is pulled low by closing a switch between the Rst pad and Gnd, to a telephone line in a manner that the modulated voltage signal is transmitted on the telephone line;

(b) connecting a telephone hand set to the same telephone line;

(c) connecting to an interactive voice response (IVR) server on the telephone network by dialing an appropriate number on the handset;

(d) entering a pin number through the telephone handset by the specific person, and pressing the switch to pull the Rst low and transmit the modulated identification sequence to the IVR;

(e) demodulating the identification sequence at the IVR, and using the demodulated identification sequence and the PIN to communicate with an authentication server and authenticate the person ~~providing a connector for connecting a smart card to a telephone;~~

~~(b) transmitting from the smart card at least an identification sequence for the user to an IVR server connected to a telephone line in the form of a modulated signal;~~

~~(c) demodulating the identification sequence at the IVR server, and~~

~~(d) authenticating the user and the transaction at an application server receiving the demodulated identification sequence from the IVR server over a communication~~

~~network wherein data processing required for generating, transmitting and authenticating the user occur without data processing assistance from the connector~~.

2. (Previously presented) The method of claim 1, wherein the identification sequence comprises at least a unique card number and a random number, the random number valid only once.

3. (Previously presented) The method as in claim 2, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

4. (Previously presented) The method as in claim 3, wherein the session key (Ki) is a function of a previous (Ki-l) emitted by the card as: Ki G(Ki-l), G is a one-way function wherein (Ki-1) is known by the authentication server.

5. (Previously presented) The method of claim 4, wherein the session key (Ki) is used by an IVR applet to encrypt a PIN entered by the user; wherein the encryption is transmitted to the authentication server along with the card number.

6. (Previously presented) The method of claim 5, wherein the authentication server decrypts the encryption code to retrieve the user PIN, using a session key deduced from the (Ki-l) stored in a database at the authentication server

7. (Previously presented) The method of claim 6, wherein the authentication is valid only if the decrypted PIN and the PIN stored in the database are identical; if this is the case, the authentication server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.

8-13. (Canceled)

14. (Currently amended) A system for authenticating ~~a user~~ and securing online transactions for a user over a telephone, comprising;

~~a connector for connecting to the telephone and the telephone connected to a telephone line;~~

a smart card having a conventional ISO 7816 six pad array and first circuitry to operate as a conventional smart card, further comprising second circuitry enabled to produce a modulated voltage signal modulated in a manner to produce an identification sequence stored on the smart card and associated with a specific person, on one otherwise unused pad once each time the Rst (reset pad) is pulled low by closing a switch between the Rst pad and Gnd, to a telephone line in a manner that the modulated voltage signal is transmitted on the telephone line ~~connected to the telephone via the connector for transmitting at least an identification sequence for the user in the form of a modulated signal~~;

a connector connecting the one pad on which the modulated signal is produced, the Gnd pad, aVbb pad, and the Rst pad of the ISO pad array to the telephone line, with a normally-open switch imposed between the Rst pad and Gnd;

a telephone connected on the telephone line;

an interactive voice response (IVR) server connected to the telephone line; and

an ~~application~~ authentication server connected to the IVR server over a communication network;

wherein upon the specific person opening a connection to the IVR by dialing an appropriate number by the handset, entering a PIN, and closing the normally open switch to cause the identification sequence to be transferred to the IVR, the IVR demodulates the identification sequence, and uses the demodulated identification sequence and the PIN to communicate with the authentication server and authenticate the person ~~the application server authenticates the user and the online transactions by receiving the demodulated identification sequence from the IVR server over a communication network and compares the received identification sequence with identification information in a database~~.

15. (Previously presented) The system of claim 14, wherein the identification sequence comprises at least a unique card number and a random number valid only once.

16. (Previously presented) The system of claim 14, wherein the random number is a session key (Ki) which is not transmitted to the application server.

17. (Previously presented) The system of claim 14, wherein a session key (Ki) is a function of a previous (Ki-l) emitted by the card such as: Ki G(Ki-l), G is a one-way function, wherein (Ki-1) is known by the application server.

18. (Previously presented) The system of claim 17, wherein the session key (Ki) is used by an IVR applet to encrypt a PIN entered by the user; said encryption is transmitted to the application server along with the card number.

19. (Previously presented) The system of claim 18, wherein the application server decrypts the encryption to retrieve the user PIN, using a session key deduced from the previous (Ki-l) stored in a database at the authentication server.

20. (Previously presented) The system of claim 19, wherein the authentication is valid only if the decrypted PIN and the PIN stored in the database are identical; if this is the case, the application server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.

21. (Previously presented) The system of claim 14, wherein the smart card is powered by the voltage provided by the telephone line.

22. (Previously presented) The system of claim 14, wherein the smart card transmits the modulated signal to the telephone line through an ISO contact.

23. (Currently amended) The system of claim 14, wherein the ~~card reader~~ connector is further integrated into the telephone handset.